# 1. Introduction

This document outlines the Asset Management Policy for [Organization Name], designed to ensure compliance with ISO/IEC 27001:2022 requirements. The policy establishes the framework for managing information assets throughout their lifecycle, ensuring their confidentiality, integrity, and availability.

# 2. Purpose

The purpose of this policy is to:

- Identify and classify all assets critical to the organization’s information security, such as hardware, software, databases, and intellectual property.

- Establish roles and responsibilities for asset management.

- Define processes for the handling, usage, and disposal of assets.

- Protect assets against unauthorized access, modification, loss, or destruction.

# 3. Scope

This policy applies to all employees, contractors, third-party vendors, and any other individuals who access or manage the organization’s information assets. It encompasses all physical and digital assets, including hardware, software, data, intellectual property, and cloud-based or third-party managed assets.

# 4. Roles and Responsibilities

- Asset Owners: Responsible for the overall management and protection of assigned assets, including classification, labeling, and inventory.

- IT Department: Ensures the implementation of technical controls for safeguarding assets and maintaining accurate asset inventories.

- Employees and Contractors: Adhere to asset management guidelines and report any incidents involving asset misuse or loss.

- Information Security Officer (ISO): Monitors compliance with this policy and ensures alignment with ISO 27001 requirements.

# 5. Asset Inventory

An up-to-date inventory of all information assets must be maintained. The inventory should include:

- Unique identifier

- Asset type (e.g., hardware, software, data)

- Owner

- Location

- Classification level

- Lifecycle status

The inventory must be reviewed at least quarterly by the IT Department, and any discrepancies should be resolved promptly.

# 6. Asset Classification

Assets must be classified based on their value, sensitivity, and criticality to the organization’s operations. The following classification levels will be used:

- Public: Information that can be freely shared without security implications (e.g., marketing materials).

- Internal: Information intended for use within the organization only (e.g., internal reports).

- Confidential: Sensitive information requiring restricted access (e.g., customer data).

- Highly Confidential: Critical information with strict access controls to prevent unauthorized disclosure (e.g., financial records, trade secrets).

# 7. Asset Labeling

All classified assets must be appropriately labeled to reflect their classification level. This labeling ensures that users handle the assets in accordance with their designated security requirements.

# 8. Asset Handling and Usage

- Access to assets must be granted on a need-to-know basis.

- All users must follow the organization’s Acceptable Use Policy when using assets.

- Portable devices and removable media must be encrypted and handled securely.

- Any sharing or transfer of assets must be authorized and documented.

# 9. Asset Maintenance

- Regular maintenance and updates must be performed on hardware and software assets, including applying patches and firmware updates within 30 days of release.

- Obsolete or unsupported assets must be identified and replaced or decommissioned within six months of becoming non-operational.

# 10. Asset Disposal

- Assets must be securely disposed of when they reach the end of their lifecycle.

- Data-bearing assets must undergo secure data destruction methods, such as degaussing, shredding, or certified wiping.

- Disposal activities must be documented and approved by the asset owner.

# 11. Incident Management

Any incidents involving the loss, theft, or unauthorized access of assets must be reported immediately to the Information Security Officer. An investigation will be conducted, and corrective actions will be implemented as necessary.

# 12. Compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract. The organization reserves the right to audit compliance with this policy at least annually as part of its internal review process.

# 13. Policy Review

This policy will be reviewed annually by the Information Security Officer or whenever there are significant changes to the organization’s operations, assets, or regulatory requirements.

# 14. Acknowledgment

All employees, contractors, and third-party vendors must acknowledge receipt and understanding of this policy. A signed acknowledgment form must be retained for audit purposes.

# Appendices

## Appendix A: Asset Inventory Template

| Asset ID | Asset Type | Owner | Location | Classification | Lifecycle Status |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## 

## Appendix B: Incident Reporting Template

| Incident ID | Date/Time | Asset Involved | Description | Actions Taken |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

## Appendix C: Policy Acknowledgment Form

I acknowledge that I have read and understood the Asset Management Policy and agree to comply with its requirements.  
  
Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 